AFFIDAVIT

I, Ryan D. Anschutz, a Task Force Officer with the Federal Bureau of Investigation (FBI), Cleveland Division, being duly sworn, depose and state as follows:

1. I have been employed as a Mansfield Police Officer for approximately ten years, and am currently assigned to the Cleveland Division, Mansfield Resident Agency's Child Exploitation Task Force. While employed by the Mansfield Police Department and assigned to the FBI, I have assisted in the investigation of federal criminal violations related to Violent Crimes and the FBI's Innocent Images National Initiative, which investigates matters involving the online sexual exploitation of children. I have gained experience through training at the FBI's Innocent Images National Initiative training center and everyday work related to conducting these types of investigations.

2. As a task force officer having received a Special Deputization from the United States Marshal's Office, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.

3. I am investigating the activities of the Internet account registered to Brittney Owens, 993 Dianewood Drive, Mansfield, Ohio 44905. As will be shown below, there is probable cause to believe that someone using the Internet account registered to Brittney Owens, has received, possessed, and/or distributed child pornography, in violation of Title 18, United States Code, Sections 2252 and 2252A. I am submitting this affidavit in support of a search warrant authorizing a search of the residence located at 993 Dianewood Drive, Ohio 44903(the "Premises"), and is more particularly described in Attachment A, for the items specified in Attachment B hereto, which items constitute instrumentalities, fruits, and evidence of the foregoing violations. I am requesting authority to search the entire Premises, including the residential dwelling and any computer and computer media located

therein where the items specified in Attachment B may be found, and to seize all items listed in Attachment B as instrumentalities, fruits, and evidence of crime.

4. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of the violation of Title 18, United States Code, Sections 2252 and 2252A, are presently located at 993 Dianewood Drive, Mansfield, Ohio 44905.

STATUTORY AUTHORITY

5. This investigation concerns alleged violations of Title 18, United States Code, Sections 2252 and 2252A, relating to material involving the sexual exploitation of minors. 18 U.S.C. § 2252(a) prohibits a person from knowingly transporting, shipping, receiving, distributing, reproducing for distribution, or possessing any visual depiction of minors engaging in sexually explicit conduct when such visual depiction was either mailed or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer. 18 U.S.C. § 2252A(a) prohibits a person from knowingly transporting, shipping, receiving, distributing, reproducing for distribution, or possessing any child pornography, as defined in 18 U.S.C. § 2256(8), when such child pornography was either mailed or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer.

DEFINITIONS

6. The following definitions apply to this Affidavit and Attachment B to this Affidavit:

a. "Child Erotica" as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

b. "Child Pornography" as used herein, includes the definition in Title 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct), as well as any visual depiction, the production of which involves the use of a minor engaged in sexually explicit conduct (see Title 18 U.S.C. §§ 2252 and 2256(2)).

c. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See Title 18 U.S.C. § 2256(5).

d. "Computer" as used herein, is defined pursuant to Title 18 U.S.C. § 1030(e)(1), as an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

e. "Computer hardware" as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

f. "Computer software" as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

g. "Computer-related documentation" as used herein, consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

h. "Computer passwords and data security devices" as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

i. "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet.

j. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants

(PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

k. “BitTorrent network” is a peer-to-peer file sharing network, accessible to and used by users world-wide.

l. "Hash Value" is a mathematical value generated by applying an algorithm to a computer file, and allows the "digital fingerprinting" of a computer file. Applying such algorithm to a digital file produces a fixed length unique identifier for that file. It is computationally infeasible for two files with different content to have the same hash values.

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

7. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

8. Child pornographers can transfer photographs from a camera onto a computer-readable format with a scanner. With a digital camera, the images can be transferred directly onto a computer. A modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world.

9. The computer’s ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution.

10. The Internet and its World Wide Web afford collectors of child pornography several different venues for obtaining, viewing and trading child pornography in a relatively secure and anonymous fashion.

11. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer in most cases.

12. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. A forensic examiner often can recover evidence suggesting whether a computer contains peer to peer software, when the computer was sharing files, and some of the files which were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data.

13. Peer to peer file sharing (P2P). P2P file sharing is a method of communication available to Internet users through the use of special software. Computers linked together through the Internet using this software form a network that allows for the sharing of digital files between users on the network. A user first obtains the P2P software, which can be downloaded from the internet. In general, P2P software allows the user to set up file(s) on a computer to be shared with others running compatible P2P software. A user obtains files by opening the P2P software on the user's computer, and conducting a search for files that are currently being shared on the network.

14. The BitTorrent network is a very popular and publically available P2P file sharing network. Most computers that are part of this network are referred to as "peers" or "clients". A peer/client can simultaneously provide files to some peers/clients while downloading files from other peers/clients.

15. The BitTorrent network can be accessed by peer/client computers via many different BitTorrent network client (software) programs, examples of which include: the BitTorrent client program; uTorrent client program; and Vuze client program, among others. These client programs are publically available and typically free P2P client software programs that can be downloaded from the Internet.

16. During the installation of typical BitTorrent network client programs, various settings are established which configure the host computer to share files via automatic uploading[1].

[1] As an example, during the downloading and installation of the publically available uTorrent client program, the license agreement for the software states the following: "Automatic Uploading". uTorrent accelerates downloads by enabling your computer to grab pieces of files from other uTorrent or BitTorrent users simultaneously. Your use of the uTorrent software to download files will, in turn, enable other users to download pieces of those files from you, thereby maximizing download speeds for all users. In uTorrent, only files that you are explicitly downloading or sharing (seeding) will be made available to others. You consent to other users' use of your network connection to download portions of such files from you. At any time, you may uninstall uTorrent through the Add/Remove Programs control panel utility. In addition, you can control uTorrent in multiple ways through its user interface without affecting any files you have already downloaded.

Typically, as users download files or pieces of files from other peers/clients on the BitTorrent network, other users (peers/clients) on the network are able to download the files or pieces of files from them, a process which maximizes the download speeds for all users on the network. Once a user has completed the download of an entire file or files, they can also continue to share the file with individuals on the BitTorrent network who are attempting to download all pieces of the file or files, a process referred to as "seeding".

17. Files or sets of files are shared on the BitTorrent network via the use of "Torrents". A "Torrent" is typically a small file that *describes* the file(s) to be shared. It is important to note that a "Torrent" does not contain the actual file(s) to be shared, but information about the file(s) to be shared needed to accomplish a download. This information includes things such as the name(s) of the file(s) being referenced in the "Torrent" and the "info hash" of the "Torrent". The "info hash" is a SHA-1[2]hash value of the set of data describing the file(s) referenced in the "Torrent". This set of data includes the SHA-1 hash value of each file piece in the torrent, the file size(s), and the file name(s). The "info hash" of each "Torrent" uniquely identifies the "Torrent" on the BitTorrent network. The "Torrent" may also contain information on how to locate file(s) referenced in the "Torrent" by identifying "Trackers". "Trackers" are computers on the BitTorrent network that collate information about the peers/clients that have recently reported they are sharing the file(s) referenced in the "Torrent" file. A "Tracker" is only a pointer to peers/clients on the network who may be

[2] The Secure Hash Algorithm (SHA) was developed by the National Institute of Standards and Technology (NIST), along with the National Security Agency (NSA), as a means of identifying files using a digital "fingerprint" that consists of a unique series of letters and numbers. The United States has adopted the SHA1 hash algorithm described herein as a Federal Information Processing Standard. SHA-1 is the most widely used of the existing SHA hash functions, and is employed in several widely used applications and protocols. A file processed by this SHA1 operation results in the creation of an associated hash value often referred to as a digital signature. SHA1 signatures provide a certainty exceeding 99.99% that two or more files with the same SHA1 signature are identical copies of the same file regardless of their file names.

sharing part or all of the file(s) referenced in the “Torrent”. “Trackers” do not actually have the file(s) but are used to facilitate the finding of other peers/clients that have the entire file(s) or at least a portion of the file(s) available for sharing. It should also be noted that the use of “Tracker(s)” on the BitTorrent network are not always necessary to locate peers/clients that have file(s) being shared from a particular “Torrent.” There are many publically available servers on the Internet that provide BitTorrent tracker services.

18. In order to locate “Torrents” of interest and download the files that they describe, a typical user will use keyword searches on torrent indexing websites, examples of which include *isohhunt.com* and the *piratebay.org.* Torrent indexing websites are essentially search engines that users on the BitTorrent network use to locate “Torrents” that describe the files they are looking to download. Torrent indexing websites do not actually host the content (files) described by “Torrents”, only the “Torrent” themselves. Once a “Torrent” is located on the website that meets a user’s keyword search criteria, the user will download the “Torrent” to their computer. The BitTorrent network client program on the user’s computer will then process that “Torrent” in order to find “Trackers” or utilize other means that will help facilitate finding other peers/clients on the network that have all or part of the file(s) referenced in the “Torrent.” It is again important to note that the actual file(s) referenced in the “Torrent” are actually obtained directly from other peers/clients on the BitTorrent network and not the “Trackers” themselves. Typically, the “Trackers” on the network return information about remote peers/clients that have recently reported they have the same file(s) available for sharing (based on SHA-1 “info hash” value comparison), or parts of the same file(s), referenced in the “Torrent”, to include the remote peers/clients Internet Protocol (IP) addresses.

19. For example, a person interested in obtaining child pornographic images or videos on the BitTorrent network can go to a torrent indexing website and conduct a keyword search using a term such as "preteen sex" or "pthc" (pre-teen hardcore). The results of the keyword search are typically returned to the user's computer by displaying them on the torrent indexing website. Based on the results of the keyword search, the user would then select a "Torrent" of interest to them to download to their computer from the website. Typically, the BitTorrent client program will then process the "Torrent." Utilizing trackers and other BitTorrent network protocols, peers/clients are located that have recently reported they have the file(s) or parts of the file(s) referenced in the "Torrent" file available for sharing. The file or files are then downloaded directly from the computer(s) sharing the file or files. Typically, once the BitTorrent network client has downloaded part of a file or files, it may immediately begin sharing the part of the file or files it has with other users on the network. The BitTorrent network client program succeeds in reassembling the file(s) from different sources only if it receives "pieces" with the exact SHA-1 hash value of that piece which is described in the "Torrent." The downloaded file or files are then stored in an area (folder) previously designated by the user and/or the client program on the user's computer or designated external storage media. The downloaded file or files, including the torrent, will remain in that location until moved or deleted by the user.

20. Law Enforcement can search the BitTorrent network in order to locate individuals sharing previously identified child exploitation material in the same way a user searches this network. To search the network for these known torrents, Law Enforcement can quickly identify targets in their jurisdiction. Law Enforcement receives this information from "Trackers" about peers/clients on the BitTorrent network recently reporting that they are involved in sharing digital files of known or suspected child pornography, based on "info

hash" SHA-1 hash values of torrents. These torrents being searched for are those that have been previously identified by law enforcement as being associated with such files.

21. There are BitTorrent network client programs which allow for single-source downloads from a computer at a single IP address, meaning that an entire file or files are downloaded only from a computer at a single IP address as opposed to obtaining the file from multiple peers/clients on the BitTorrent network. This procedure allows for the detection and investigation of those computers involved in sharing digital files of known or suspected child pornography on the BitTorrent network.

22. During the query and/or downloading process from a suspect BitTorrent network client, certain information may be exchanged between the investigator's BitTorrent client program and the suspect client program they are querying and/or downloading a file from. This information includes: 1) The suspect client's IP address; 2) A confirmation from the suspect client that they have pieces of the file(s) being requested, in whole or in part, and that the pieces of the file(s) is being reported as shared from the suspect client program; and 3) The BitTorrent network client program and version being utilized by the suspect computer. Third party software available to law enforcement has the ability to log this information.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

23. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally difficult to accomplish this kind of data search on site; and

b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

24. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit (CPU). In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media).

25. In addition, there is probable cause to believe that the computer and its storage devices are instrumentalities of the crime(s), within the meaning of Title 18 U.S.C. §§ 2251 through 2256, and should all be seized as such.

BACKGROUND OF THE INVESTIGATION

26. On several occasions between August 19th, 2016 and September 15th, 2016, TFO Ryan D. Anschutz, while connected to the Internet in an online covert capacity, was signed into an automated software program which operates on the BitTorrent platform. The software program automates the process of browsing and downloading files form a single source. The downloaded torrents are shared by a user over the BitTorrent network. The software program searches the BitTorrent network for torrents of interest with infohash values of suspected child pornography. During the aforementioned time period TFO Anschutz connected to the individual utilizing IP address 76.188.17.160 on twenty one (21) separate occasions for single source download of torrents of interest with infohash values suspected of child pornography.

27. On September 15th, 2016, the individual utilizing IP address 76.188.17.160 was reporting to have, and making available for sharing, 4669 files referenced by a torrent of interest with an infohash: 8b687670eb33dbfd3f386a5f4466262477f7e22f. Several of these files were identified as being a file of investigative interest. The individual utilizing IP address 76.188.17.160 was using BitTorrent client software –UT3480- uTorrent 3.4.8.

28. TFO Anschutz successfully downloaded seven hundred ten (710) files from the torrent that computer at IP address 76.188.17.160 was making available. Approximately six hundred fifty four (654) of those files were identified as child pornography and five of those files that were identified as child pornography are described below:

a) Image Title: up_carols_arse.jpg

V6VBCHS46Z2HIX4ITRYRYB466GHFMY63

Description: The image depicts a prepubescent female laying on a blanket with her legs spread exposing her genitalia. A male subject, with his penis exposed is observed engaging in genital to anal intercourse with the female toddler.

b) Image Title: Pthc – Qqaazz 1yo – Pedo man pudding a chubby baby puss (cute).jpg

O6QZGVKYJ33AKQY7LNQFBLA6SH7WN

Description: The image depicts a nude toddler female laying on her back with her legs spread exposing her genitalia. An adult male is observed with his penis exposed, pressing the penis on/into the toddler vagina with what appears to be male ejaculate around the genitalia.

c) Image Title: goldi_tied+and+hanging.jpg

KSAHDJFM3GEX665Z22HSBVDBMEBJVNQH

Description: The image depicts a nude female toddler hanging upside down with a black bandana around her mouth. There is also a rope wrapped around the toddler and a Sharpie inserted in her vagina.

d) Image Title: 20050601083743.jpg

TVZALZKBIWMQW4DRG33MOYFKII3KCUHX

Description: The image depicts a nude male toddler and a nude adult male engaged in oral to genital intercourse.

e) Image Title: Baby child H7x 1563.jpg

THQ6EHV6PKFOOCYSOPJRZG7XLFRDY5IA

Description: The image depicts an adult female and a nude male toddler engaged in oral to genital intercourse.

29. On September 21, 2016 TFO Anschutz queried the IP address 76.188.17.160 through the American Registry for Internet Numbers (ARIN), which reported that this IP address was registered to Time Warner Cable. Results from administrative subpoenas sent to Time Warner Cable for the dates and times that the above-described files were downloaded revealed that at those days and times, the IP address was assigned to the account registered to Brittney Owens at 993 Dianewood Drive, Mansfield, Ohio 44903, telephone number 419-565-9658.

30. I searched various records indices for information regarding Brittney Owens at the address 993 Dianewood Drive, Mansfield, Ohio 44903.

b. Ohio Bureau of Motor Vehicle records reports accessed through the Ohio Law Enforcement Gateway (OHLEG) database, which can be accessed and searched by affiant, for Brittney Owens, shows a valid Ohio driver's license with an active address of 993 Dianewood Drive, Mansfield, Ohio 44903.

31. On October 5th, 2016, a physical surveillance of 993 Dianewood Drive, Mansfield, Ohio 44903 was conducted. The property is located on the north side of Dianewood Drive and is described as a two story multiple family dwelling with brick walls, white trim, white screen door and a white interior front door. 993 is observed to be the east side of the structure. The garage is located in the rear bottom of the residence and the number 993 is located on the east side white support post of the front porch.

CONCLUSION

32. Based on the aforementioned factual information, your affiant respectfully submits that there is probable cause to believe that an individual who resides at the residence described above is involved in possession and distribution of child pornography. Your affiant respectfully submits that there is probable cause to believe that an individual residing in the residence described above has violated Title 18 U.S.C. §§ 2252 and 2252A. Additionally, there is probable cause to believe that evidence of the commission of criminal offenses, namely, violations of 18 U.S.C. §§ 2252 and 2252A, is located in the residence described above, and this evidence, listed in Attachment B of this affidavit, which is incorporated herein by reference, is contraband, the fruits of crime, or things otherwise criminally possessed, or property which is or has been used as the means of committing the foregoing offenses.

33. Your affiant, therefore, respectfully requests that the attached warrant be issued authorizing the search and seizure of the items listed in Attachment B.

Ryan D. Anschutz
Task Force Officer
Federal Bureau of Investigation

Sworn and subscribed before me this 11th Day of October, 2016

HONORABLE THOMAS M. PARKER
UNITED STATES MAGISTRATE JUDGE